

**THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS**

ERIC FLORENCE and AISHA BUNDAGE,

on behalf of themselves and all others
similarly situated,

Plaintiffs,

v.

ORDER EXPRESS, INC.,

Defendant.

Case No.: 1:22-cv-07210

**AMENDED CLASS ACTION
COMPLAINT**

DEMAND FOR JURY TRIAL

Plaintiffs Eric Florence and Aisha Bundage (“Plaintiffs”) bring this Amended Class Action Complaint against Order Express, Inc. (“Defendant”), individually and on behalf of all others similarly situated (“Class Members”), and alleges, upon personal knowledge as to their own actions and their counsels’ investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personal identifiable information (“PII”)¹ of more than 63,000 individuals, including, but not limited to, name, Social Security number, and driver’s license number.

2. According to Defendant’s website, its “primary activity [is] the fast and secure sending of money.”²

3. Prior to and through September 7, 2022, Defendant obtained the PII of Plaintiffs

¹ Personally identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

² See <https://www.orderexpress.com.mx/Home/about-us/> (last visited Dec. 20, 2022).

and Class Members, including by collecting it directly from Plaintiffs and Class Members.

4. Prior to and through September 7, 2022, Defendant stored the PII of Plaintiffs and Class Members, unencrypted, in an Internet-accessible environment on Defendant's network.

5. On or before September 7, 2022, Defendant learned of a data breach on its network that occurred from July 29, 2022 to September 7, 2022 (the "Data Breach").

6. Defendant determined that, during the Data Breach, an unknown actor may have accessed and/or acquired the PII of Plaintiffs and Class Members.

7. On or around October 20, 2022, reports began surfacing on the Internet that Defendant had been the subject of a ransomware attack by the "CL0P" ransomware family and that information obtained during the attack had surfaced on the dark web.³

8. One website reported that the "[e]xfiltrated data type" included "[i]nformation about many people, business process and practice," that the "[l]eaked data" included "[s]ample with screenshots of PII documents," and that the "[r]ansom deadline" was September 19, 2023.⁴

9. Another website reported that, in connection with the Data Breach, "43M lines were advertised for sale which includes the address, names, and phone numbers, orders made (SSN 32M lines in total), ID's, DL payment info and much more" and "Total file size: Customer data 6GB; Company data 87GB."⁵ This website also included a screenshot of this advertisement, which further stated that "1M sample will be provided here a lot of info will be removed from the samples."⁶

10. In other words, a ransom was demanded, and six gigabytes of customer data was

³ See <https://www.breachsense.io/breaches/order-express/> (last visited Feb. 27, 2023).

⁴ See <https://hackmanac.com/news/hacks-of-the-day-08-01-2023> (last visited Feb. 27, 2023).

⁵ See <https://www.cyfirma.com/news/weekly-intelligence-report-10-feb-2023/> (last visited Feb. 27, 2023).

⁶ *Id.*

advertised for sale on the dark web, including address, names, phone numbers, orders made, Social Security numbers, ID's, driver's license payment info, and "much more."

11. On or around December 15, 2022, Defendant began notifying various states Attorneys General of the Data Breach.

12. On or around December 15, 2022, Defendant began notifying Plaintiffs and Class Members of the Data Breach.

13. The notices that Defendant sent to various states Attorneys General and to Plaintiffs and Class Members did not disclose that (i) Plaintiffs' and Class Members' PII was actually acquired by an unauthorized actor during the Data Breach, (ii) the PII was the subject of a ransom demand with a ransom deadline of September 19, 2023, and (iii) the PII had been made available for sale on the dark web.

14. By obtaining, collecting, using, and deriving a benefit from the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion. Defendant admits that the unencrypted PII that may have been accessed and/or acquired by an unauthorized actor included name, Social Security number, and driver's license number.

15. The exposed PII of Plaintiffs and Class Members can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Plaintiffs and Class Members now face a lifetime risk of (i) identity theft, which is heightened here by the loss of Social Security numbers, and (ii) the sharing and detrimental use of their sensitive information.

16. The PII was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect the PII of Plaintiffs and Class Members. In addition to

Defendant's failure to prevent the Data Breach, Defendant waited more than three months after the Data Breach occurred to report it to the states Attorneys General and affected individuals. Defendant has also purposefully maintained secret the specific vulnerabilities and root causes of the breach and has not informed Plaintiffs and Class Members of that information.

17. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm, including the sharing and detrimental use of their sensitive information. The risk will remain for their respective lifetimes.

18. Plaintiffs bring this action on behalf of all persons whose PII was compromised as a result of Defendant's failure to: (i) adequately protect the PII of Plaintiffs and Class Members; (ii) warn Plaintiffs and Class Members of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

19. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, (iv) the disclosure of their private information, and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

20. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that the PII of Plaintiffs and Class Members was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII of Plaintiffs and Class Members was compromised through disclosure to an unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

21. Plaintiff Florence is a citizen of California residing in San Leandro, California.

22. Plaintiff Bundage is a citizen of Texas residing in Houston, Texas.

23. Defendant is an Illinois corporation with a principal place of business in Chicago, Illinois.

24. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

25. All of Plaintiffs' claims stated herein are asserted against Defendant and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

26. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum

or value of \$5 million, exclusive of interest and costs, there are more than 100 members in the proposed class, and at least one Class Member, including Plaintiff, is a citizen of a state different from Defendant to establish minimal diversity.

27. Defendant is a citizen of Illinois because it is a corporation formed under Illinois law with its principal place of business in Chicago, Illinois.

28. The Northern District of Illinois has personal jurisdiction over Defendant because it conducts substantial business in Illinois and this District and collected and/or stored the PII of Plaintiffs and Class Members in this District.

29. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant operates in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District, including Defendant collecting and/or storing the PII of Plaintiffs and Class Members.

IV. FACTUAL ALLEGATIONS

Background

30. Defendant collected the PII of Plaintiffs and Class Members and stored it, unencrypted, on Defendant's internet-accessible network.

31. Plaintiffs and Class Members relied on this sophisticated Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiffs and Class Members demand security to safeguard their PII.

32. Defendant had a duty to adopt reasonable measures to protect the PII of Plaintiffs and Class Members from involuntary disclosure to third parties.

The Data Breach

33. On or about December 15, 2022, Defendant sent Plaintiffs and Class Members a *Notice of Data Breach* and submitted sample notices to various states' Attorneys General. Defendant informed Plaintiffs and other Class Members that:

What Happened? On September 7, 2022, we discovered unusual activity on our computer network and immediately began an investigation, which included working with third-party specialists. The investigation determined an unknown party accessed parts of our computer network without authorization between July 29, 2022 and September 7, 2022. Therefore, we conducted a review of our network to determine the type of information contained therein and to whom the information related. On November 18, 2022, we completed our review and began confirming address information for potentially impacted individuals.

What Information Was Involved? The information identified in our review included identification information you may have provided to us, including your name in combination with one or more of the following: <<Compromised Data Elements Specific to Letter Recipient>>.⁷

34. The *Notice of Data Breach* that Defendant sent to Plaintiff Florence stated that his driver's license number was impacted during the Data Breach.

35. Defendant reported to the Attorney General of Massachusetts that Social Security numbers and driver's license numbers were impacted in the Data Breach.

36. Defendant admitted in the sample *Notice of Data Breach* and the sample notices and reports it sent to the states' Attorneys General that an unauthorized actor accessed sensitive information about Plaintiffs and Class Members, including name, Social Security number, and driver's license number.

37. In response to the Data Breach, Defendant claims that it "conducted an investigation and took additional steps to further secure our network."⁸

⁷ Exhibit 1 (sample Notice of Data Breach filed with Maine Attorney General).

⁸ *Id.*

38. However, the details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur again have not been shared with regulators or Plaintiffs and Class Members, who retain a vested interest in ensuring that their information remains protected.

39. The unencrypted PII of Plaintiffs and Class Members has ended up for sale on the dark web, and may fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members. Unauthorized individuals can easily access the PII of Plaintiffs and Class Members.

40. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiffs and Class Members, causing the exposure of PII for Plaintiffs and Class Members.

41. Because Defendant had a duty to protect Plaintiffs' and Class Members' PII, Defendant should have accessed readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

42. In the years immediately preceding the Data Breach, Defendant knew or should have known that Defendant's computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

43. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care

organizations, industrial companies, and the transportation sector.”⁹

44. In April 2020, ZDNet reported, in an article titled “Ransomware mentioned in 1,000+ SEC filings over the past year,” that “[r]ansomware gangs are now *ferociously aggressive in their pursuit of big companies*. They breach networks, use specialized tools to maximize damage, *leak corporate information on dark web portals*, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay.”¹⁰

45. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a “Ransomware Guide” advising that “[m]alicious actors have *adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data* if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.”¹¹

46. This readily available and accessible information confirms that, prior to the Data Breach, Defendant knew or should have known that (i) cybercriminals were targeting big companies such as Defendant, (ii) cybercriminals were ferociously aggressive in their pursuit of big companies such as Defendant, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals’ tactics included threatening to release stolen data.

47. In light of the information readily available and accessible on the internet before

⁹ FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), available at <https://www.ic3.gov/Media/Y2019/PSA191002> (last visited Jan. 25, 2022).

¹⁰ ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), available at <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/> (last visited Jan. 25, 2022).

¹¹ U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS_ISAC_Ransomware%20Guide_S508C_.pdf (last visited Jan. 25, 2022).

the Data Breach, Defendant, having elected to store the unencrypted PII of Plaintiffs and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII and Defendant's type of business had cause to be particularly on guard against such an attack.

48. Prior to the Data Breach, Defendant knew or should have known that there was a foreseeable risk that Plaintiffs' and Class Members' PII could be accessed, exfiltrated, and published as the result of a cyberattack.

49. Prior to the Data Breach, Defendant knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Defendant Acquires, Collects, and Stores the PII of Plaintiffs and Class Members.

50. Defendant acquired, collected, and stored the PII of Plaintiffs and Class Members.

51. By obtaining, collecting, and storing the PII of Plaintiffs and Class Members, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

52. Plaintiffs and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendant to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

53. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."¹²

¹² See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited Aug. 23, 2021).

54. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.¹³

55. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it....
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software,

¹³ *Id.* at 3-4.

firewalls, and email filters—and keep them updated—to reduce malicious network traffic....¹⁴

56. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection

¹⁴ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* <https://us-cert.cisa.gov/ncas/tips/ST19-001> (last visited Aug. 23, 2021).

- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁵

57. Given that Defendant was storing the PII of more than 63,000 individuals, Defendant could and should have implemented all of the above measures to prevent and detect ransomware attacks.

58. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of more than 63,000 individuals, including Plaintiffs and Class Members.

Securing PII and Preventing Breaches

59. Defendant could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiffs and Class Members. Alternatively, Defendant could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

60. Defendant's negligence in safeguarding the PII of Plaintiffs and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

61. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII of Plaintiffs and Class Members from being compromised.

62. The Federal Trade Commission ("FTC") defines identity theft as "a fraud

¹⁵ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited Aug. 23, 2021).

committed or attempted using the identifying information of another person without authority.”¹⁶ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹⁷

63. The ramifications of Defendant’s failure to keep secure the PII of Plaintiffs and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

64. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹⁸ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹⁹ Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.²⁰

¹⁶ 17 C.F.R. § 248.201 (2013).

¹⁷ *Id.*

¹⁸ *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Jan. 26, 2022).

¹⁹ *Here’s How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed Jan. 26, 2022).

²⁰ *In the Dark*, VPNOOverview, 2019, available at: <https://vpnooverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Dec. 29, 2020).

65. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to “close” and difficult, if not impossible, to change.

66. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market.”²¹

67. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

68. The fraudulent activity resulting from the Data Breach may not come to light for years.

69. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.²²

²¹ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed Jan. 26, 2022).

²² *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed Mar. 15, 2021).

70. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiffs and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendant's data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

71. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

72. Defendant was, or should have been, fully aware of the unique type and the significant volume of data contained in Defendant's contract search tool, amounting to potentially tens of thousands of individuals' detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

73. To date, Defendant has offered Plaintiffs and Class Members only two years of credit monitoring and identity theft protections services through Equifax. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

74. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Plaintiffs and Class Members.

Plaintiff Florence's Experience

75. Plaintiff Florence used Defendant to send and/or receive funds prior to the Data Breach and received Defendant's *Notice of Data Breach*, dated December 15, 2022, on or about that date. The notice stated that Plaintiff Florence's personal information, including driver's

license number, may have been accessed and/or acquired by an unauthorized actor.

76. As a result of the Data Breach, Plaintiff Florence's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Florence's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff Florence will have to worry about when and how his sensitive information may be shared or used to his detriment.

77. As a result of the Data Breach notice, Plaintiff Florence spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach* and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

78. Additionally, Plaintiff Florence is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

79. Plaintiff Florence stores any documents containing his sensitive PII in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

80. Plaintiff Florence suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

81. Plaintiff Florence has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his driver's license number, being placed in the hands of unauthorized third parties and possibly criminals.

82. Plaintiff Florence has a continuing interest in ensuring that his PII, which, upon

information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff Bundage's Experience

83. Plaintiff Bundage used Defendant to send and/or receive funds prior to the Data Breach and received Defendant's *Notice of Data Breach*, dated December 15, 2022, on or about that date. The notice stated that Plaintiff Bundage's personal information, including Social Security number or tax identification number, may have been accessed and/or acquired by an unauthorized actor.

84. As a result of the Data Breach, Plaintiff Bundage's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff Bundage's sensitive information has been irreparably harmed. For the rest of her life, Plaintiff Bundage will have to worry about when and how her sensitive information may be shared or used to her detriment.

85. As a result of the Data Breach notice, Plaintiff Bundage spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the *Notice of Data Breach* and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

86. Additionally, Plaintiff Bundage is very careful about sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

87. Plaintiff Bundage stores any documents containing her sensitive PII in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for his various online accounts.

88. Plaintiff Bundage suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

89. Plaintiff Bundage has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially her Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

90. Plaintiff Bundage has a continuing interest in ensuring that her PII, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

91. Plaintiffs bring this nationwide class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

92. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

All individuals whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and Class Members on or around December 15, 2022 (the "Nationwide Class").

93. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiffs assert claims on behalf of a separate subclass, defined as follows:

All individuals who used Defendant to send and/or receive funds on or before September 7, 2022, and whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and Class Members on or around December 15, 2022 (the "Customers Subclass").

94. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Florence asserts claims on behalf of a separate statewide subclass,

defined as follows:

All individuals who are residents of California and whose PII may have been accessed and/or acquired in the data incident that is the subject of the Notice of Data Breach that Defendant sent to Plaintiffs and Class Members on or around December 15, 2022 (the “California Subclass”) (collectively, with the Nationwide Class and the Customers Subclass, “the Classes”).

95. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

96. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

97. Numerosity, Fed R. Civ. P. 23(a)(1): The Classes are so numerous that joinder of all members is impracticable. Defendant reported to the Maine attorney general that 63,220 individuals were impacted in the Data Breach, and the Classes are apparently identifiable within Defendant’s records.

98. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class Members;
- b. Whether Defendant had duties not to disclose the PII of Plaintiffs and Class Members

to unauthorized third parties;

- c. Whether Defendant had duties not to use the PII of Plaintiffs and Class Members for non-business purposes;
- d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class Members;
- e. When Defendant actually learned of the Data Breach;
- f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and Class Members that their PII had been compromised;
- g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII had been compromised;
- h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;
- k. Whether Plaintiffs and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendant's wrongful conduct;
- l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and
- m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

99. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

100. Policies Generally Applicable to the Classes: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Classes, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Classes as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Classes as a whole, not on facts or law applicable only to Plaintiff.

101. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Classes. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Classes and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

102. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require.

Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

103. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Classes and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

104. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

105. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

106. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act

unlawfully as set forth in this Complaint.

107. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

108. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- c. Whether Defendant failed to comply with its own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;
- e. Whether Defendant breached the implied contract;
- f. Whether Defendant adequately and accurately informed Plaintiffs and Class Members that their PII had been compromised;
- g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

- h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members; and,
- i. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendant's wrongful conduct.

COUNT I
NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class)

109. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 108.

110. Defendant has full knowledge of the sensitivity of the PII and the types of harm that Plaintiffs and the Nationwide Class could and would suffer if the PII were wrongfully disclosed.

111. Defendant knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiffs and the Nationwide Class involved an unreasonable risk of harm to Plaintiffs and the Nationwide Class, even if the harm occurred through the criminal acts of a third party.

112. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that the PII of Plaintiffs and the Nationwide Class in Defendant's possession was adequately secured and protected.

113. Defendant also had a duty to exercise appropriate clearinghouse practices to remove from an Internet-accessible environment the PII it was no longer required to retain pursuant to regulations and had no reasonable need to maintain in an Internet-accessible environment.

114. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of the PII of Plaintiffs and the Nationwide Class.

115. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and the Nationwide Class. That special relationship arose because Defendant acquired Plaintiffs' and the Nationwide Class's confidential PII in the course of its business practices.

116. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or the Nationwide Class.

117. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Nationwide Class was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

118. Plaintiffs and the Nationwide Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the inherent risks in collecting and storing the PII of Plaintiffs and the Nationwide Class, the critical importance of providing adequate security of that PII, and the necessity for encrypting PII stored on Defendant's systems.

119. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and the Nationwide Class. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiffs and the Nationwide Class, including basic encryption techniques freely available to Defendant.

120. Plaintiffs and the Nationwide Class had no ability to protect their PII that was in,

and possibly remains in, Defendant's possession.

121. Defendant was in a position to protect against the harm suffered by Plaintiffs and the Nationwide Class as a result of the Data Breach.

122. Defendant had and continue to have a duty to adequately disclose that the PII of Plaintiffs and the Nationwide Class within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Nationwide Class to (i) take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties and (ii) prepare for the sharing and detrimental use of their sensitive information.

123. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII of Plaintiffs and the Nationwide Class.

124. Defendant has admitted that the PII of Plaintiffs and the Nationwide Class was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

125. Defendant, through its actions and/or omissions, unlawfully breached its duties to Plaintiffs and the Nationwide Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiffs and the Nationwide Class during the time the PII was within Defendant's possession or control.

126. Defendant improperly and inadequately safeguarded the PII of Plaintiffs and the Nationwide Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

127. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect the PII of Plaintiffs and the Nationwide Class in the face of increased risk of theft.

128. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and the Nationwide Class by failing to have appropriate procedures in place to detect and prevent dissemination of the PII.

129. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove from the Internet-accessible environment any PII it was no longer required to retain pursuant to regulations and which Defendant had no reasonable need to maintain in an Internet-accessible environment.

130. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and the Nationwide Class the existence and scope of the Data Breach.

131. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and the Nationwide Class, the PII of Plaintiffs and the Nationwide Class would not have been compromised.

132. There is a close causal connection between Defendant's failure to implement security measures to protect the PII of Plaintiffs and the Nationwide Class and the harm, or risk of imminent harm, suffered by Plaintiffs and the Nationwide Class. The PII of Plaintiffs and the Nationwide Class was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures.

133. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; (iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention,

detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII of Plaintiffs and the Nationwide Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and the Nationwide Class.

134. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

135. Additionally, as a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class have suffered and will suffer the continued risks of exposure of their PII, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII in its continued possession.

136. As a direct and proximate result of Defendant's negligence, Plaintiffs and the Nationwide Class are entitled to recover actual, consequential, and nominal damages.

COUNT II
BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Customer Subclass)

137. Plaintiffs and the Customer Subclass re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 108.

138. In using Defendant to send and/or receive funds, Plaintiffs and the Customer Subclass provided and entrusted their PII to Defendant.

139. Defendant required Plaintiffs and the Customer Subclass to provide and entrust their PII as condition of using Defendant to send and/or receive funds.

140. As a condition of using Defendant to send and/or receive funds, Plaintiffs and the Customer Subclass provided and entrusted their PII. In so doing, Plaintiffs and the Customer Subclass entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such PII, to keep such PII secure and confidential, and to timely and accurately notify Plaintiffs and the Customer Subclass if their PII had been compromised or stolen.

141. Plaintiffs and the Customer Subclass fully performed their obligations under the implied contracts with Defendant.

142. Defendant breached the implied contracts it made with Plaintiffs and the Customer Subclass by failing to implement appropriate technical and organizational security measures designed to protect their PII against accidental or unlawful unauthorized disclosure or unauthorized access and otherwise failing to safeguard and protect their PII and by failing to provide timely and accurate notice to them that PII was compromised as a result of the data breach.

143. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Customer Subclass have suffered (and will continue to suffer) the threat of the sharing and detrimental use of their confidential information; ongoing, imminent, and

impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

144. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and the Customer Subclass are entitled to recover actual, consequential, and nominal damages.

COUNT III
DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class)

145. Plaintiffs and the Nationwide Class re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 108.

146. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

147. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiffs' and the Nationwide Class's PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and the Nationwide Class from further data breaches that compromise their PII. Plaintiffs alleges that Defendant's data security measures remain inadequate. Defendant publicly denies these allegations. Furthermore, Plaintiffs continues

to suffer injury as a result of the compromise of their PII and remain at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendant has undertaken in response to the Data Breach.

148. Plaintiffs and the Nationwide Class's have an ongoing, actionable dispute arising out of Defendant's inadequate security measures, including (i) Defendant's failure to encrypt Plaintiffs' and the Nationwide Class's PII, including Social Security numbers, while storing it in an Internet-accessible environment and (ii) Defendant's failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security number of Plaintiff.

149. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendant owes a legal duty to secure the PII of Plaintiffs and the Nationwide Class;
- b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and
- c. Defendant's ongoing breaches of its legal duty continue to cause Plaintiffs harm.

150. This Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendant to:

- d. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;

- e. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;
- f. regularly test its systems for security vulnerabilities, consistent with industry standards;
- g. implement an education and training program for appropriate employees regarding cybersecurity.

151. If an injunction is not issued, Plaintiffs will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

152. The hardship to Plaintiffs if an injunction is not issued exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

153. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendant, thus eliminating the additional injuries that would result to Plaintiffs and others whose confidential information would be further compromised.

COUNT IV
Violations of California's Consumer Privacy Act,
Cal. Civ. Code § 1798.100, *et seq.* ("CCPA")
(On Behalf of Plaintiffs Peoples and Brooks and the California Subclass)

154. Plaintiff Florence and the California Subclass re-allege and incorporate paragraphs 1-108 as if fully set forth herein.

155. Defendant violated section 1798.150(a) of the CCPA, Cal. Civ. Code § 1798.150(a), by failing to prevent Plaintiff Florence's and the California Subclass's PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the PII.

156. The PII of Plaintiff Florence and the California Subclass was subjected to unauthorized access and exfiltration, theft, or disclosure as a direct and proximate result of Defendant's violations of its duty under the CCPA.

157. Plaintiff Florence and the California Subclass lost money or property, including but not limited to the loss of legally protected interest in the confidentiality and privacy of their PII, nominal damages, and additional losses as a direct and proximate result of Defendant's acts described above.

158. Defendant knew, or should have known, that its network computer systems and data security practices were inadequate to safeguard PII and that the risk of a data breach or theft was highly likely. Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect PII, such as properly encrypting the PII so in the event of a data breach an unauthorized third party cannot read the PII. As a result of the failure to implement reasonable security procedures and practices, the PII of Plaintiff Florence and members of the California Subclass was exposed.

159. Defendant is organized for the profit or financial benefit of its owners and collects PII as defined in Cal. Civ. Code § 1798.140.

160. Defendant has a gross annual revenue of over \$25 million and buys, receives, or sells the personal information of 50,000 or more California residents, households, or devices.

161. Plaintiff Florence and California Subclass members seek relief under § 1798.150(a), including, but not limited to, recovery of actual damages; injunctive or declaratory relief; any other relief the court deems proper; and attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5). Pursuant to Section 1798.150(b) of the CCPA, Plaintiff Florence gave written notice to Defendant of its violations of section 1798.150(a) by certified mail sent on or before January 3, 2023.

162. Defendant, however, failed to "actually cure" its violations within 30 days of the written notice, and failed, pursuant to § 1798.150(b) to "provide[] the consumer an express written statement that the violations have been cured and that no further violations shall occur."

163. Defendant failed to "actually cure" its violations by, among other things, not encrypting Plaintiff Florence's and the California Subclass's PII and by not deleting Plaintiff Florence's and the California Subclass's PII it no longer had a reasonable need to maintain in an Internet accessible environment.

164. As a result, Plaintiff Florence and California Subclass members seek relief under § 1798.150(a), including, but not limited to, statutory damages in an amount not less than one hundred dollars (\$100) and not greater than seven hundred and fifty (\$750) per consumer per incident or actual damages, whichever is greater; injunctive or declaratory relief; any other relief the Court deems proper; and attorneys' fees and costs pursuant to Cal. Code Civ. Proc. § 1021.5.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and Class Members, request judgment against Defendant and that the Court grant the following:

- A. For an Order certifying the Nationwide Class, the Customer Subclass, and the California Subclass and appointing Plaintiffs and their Counsel to represent such Classes;
- B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiffs and Class Members, and from refusing to issue prompt, complete, any accurate disclosures to Plaintiffs and Class Members;
- C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:
 - i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;
 - ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;
 - iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;
 - iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiffs and Class Members;
 - v. prohibiting Defendant from maintaining the PII of Plaintiffs and Class

Members on a cloud-based database;

- vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;
- vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;
- viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;
- ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;
- x. requiring Defendant to conduct regular database scanning and securing checks;
- xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;
- xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a

breach;

- xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;
- xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;
- xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;
- xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the Classes, and to report any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, and nominal damages,

as allowed by law in an amount to be determined;

- E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;
- F. For prejudgment interest on all amounts awarded; and
- G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: March 2, 2023

Respectfully Submitted,

/s/ Ryan D. Maxey

Michael N. Hanna

N.D. IL Bar No. 85035 (FL)

Morgan & Morgan, P.A.

55 E Monroe St. Ste. 3800

Chicago, IL 60603

2000 Town Center, Suite 1900

Southfield, MI 4807

(313) 739-1950

mhanna@forthepeople.com

Ryan D. Maxey

MORGAN & MORGAN COMPLEX

BUSINESS DIVISION

201 N. Franklin Street, 7th Floor

Tampa, Florida 33602

(813) 223-5505

jyanchunis@ForThePeople.com

rmaxey@ForThePeople.com

Attorneys for Plaintiffs and the Proposed Class

CERTIFICATE OF SERVICE

I, the undersigned, do hereby certify that on March 2, 2023, a copy of the foregoing document was filed electronically. Notice of this filing will be sent to counsel of record by operation of the Court's electronic filing system.

/s/ Ryan D. Maxey

Ryan D. Maxey